



21W
ATP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Ulf Dahl
Serial No. : 09/840,188
Filed : April 24, 2001
Title : DATA SECURITY SYSTEM FOR A DATABASE

Art Unit : 2132
Examiner : Jung W. Kim

Mail Stop Appeal Brief - Patents

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

(1) Real Party in Interest

The real party in interest is Protegrity Corporation, a corporation organized under the laws of the Cayman Islands, having a place of business at P.O. Box 309, Ugland House, South Church Street, Grand Cayman, Cayman Islands. This assignment has not yet been recorded.

(2) Related Appeals and Interferences

Neither Appellant, nor Appellant's legal representative, nor the assignee are aware of any appeals or interferences that will directly affect or be affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

Claims 18-54 and 56-92 are pending. Claims 1-17, 55, and 93 were canceled. Claims 18, 19, 21, 28, 29, 31, 33, 37, 41, 42, 48, 49, 56, 57, 59, 66-68, 70, 74, 75, 79, 80, 86, 87, and 94-99 are rejected as rendered obvious by *Thomson*, U.S. Patent No. 5,751,949, in view of *Denning*, "Field Encryption and Authentication." Claims 20, 22, 43, 50, 58, 60, 81 and 88 are rejected as rendered obvious by *Thomson* in view of *Denning* and in further view of *Charles P. Pfleeger*,

CERTIFICATE OF MAILING BY FIRST CLASS MAIL

I hereby certify under 37 CFR §1.8(a) that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

02/03/2006 MAHRED1 00000029 09840188

01 FC:2402

250.00 OP

January 30, 2006

Date of Deposit

Signature

Kate A. Niejadlik

Typed or Printed Name of Person Signing Certificate

“Security in Computing,” Englewood Cliffs, New Jersey: P T R Prentice-Hall, 1989. Claims 23-27, 34-36, 38-40, 45-47, 52-54, 61 -65, 71 -73, 76-78, 83-85 and 90-92 are rejected as rendered obvious by *Thomson* in view of *Denning* and in further view of *Gaskell et al.*, “Improved Security for Smart Card Use in DCE,” February, 1995, Open Software Foundation, Request For Comments 71.0. Claim 30 is rejected as rendered obvious by *Thomson* in view of *Denning* and in further view of *Johansson et al.*, International Publication No. WO 95115628. Claims 32, 44, 51, 69, 82 and 89 are rejected as rendered obvious by *Thomson* in view of *Denning* and in further view of *Abraham et al.*, U.S. Patent No. 5,148,481.

Each of the rejections is appealed.

Claims 18, 41, 56, 79, and 86 are independent.

(4) Status of Amendments

No claims were amended subsequent to final rejection.

(5) Summary of Claimed Subject Matter

The claimed subject matter relates broadly to enhancing database security through encryption. The disclosure explains that so-called “shell security” is sometimes inadequate because it may be bypassed by a malicious user.¹ To resolve this problem, the application teaches “an improved method for processing information, by means of which it is possible to increase the protection against unauthorized access to sensitive information.”²

The specification provides an example of the claimed invention, in which data, some of which is encrypted, is stored in certain cells in a database O-DB. In a second database, IAM-DB, is stored a data element protection catalogue containing protection attributes with processing rules for each of the data elements in O-DB.³ The specification explains that the protection attributes may include rules indicating how to process a particular data element in O-DB, or rules indicating that information about how to process the particular data element may be found in

¹ *Specification*, 2:31-3:11.

² *Specification*, 3:14-18.

³ *Specification*, 4:1-13.

some other location.⁴ The specification provides further examples of information that may be contained in the data protection catalogue: an indication of the strength of encryption to be used for a given data element; an indication of the strength of encryption to be used if a given data element is to be transmitted over a network; an indication of what programs are authorized to access a given data element; an indication of the owner of a given data element; an indication of when a particular data element expires; and an indication as to whether the system should log events pertaining to processing the data element.⁵

Independent claim 18 recites a data processing method comprising maintaining a database containing a table of data in row and column format,⁶ at least a portion of the data being encrypted⁷; maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table;⁸ and controlling access to the specified proper subset of data in the table according to the separately maintained information.⁹

Dependent claim 23 recites the method of claim 18, wherein controlling access to the specified proper subset of the data comprises using a tamper-resistant hardware module.¹⁰

Dependent claim 32 recites the method of claim 18, wherein the information for controlling access comprises encrypted information.¹¹

Independent claim 41 recites a method comprising providing a database containing a table having at least two columns of data;¹² encrypting data in a first column using first cryptographic information;¹³ encrypting data in a second column using second cryptographic information;¹⁴ storing the first and second cryptographic information outside of the table;¹⁵ controlling access to data in the first column using the first cryptographic information stored

⁴ *Specification*, 4:2-13.

⁵ *Specification*, 7:30-8:21.

⁶ *Specification*, FIG. 4 ("O-DB"); 4:1-5; 5:1 (table).

⁷ *Specification*, 4:3.

⁸ *Specification*, 4:8-13.

⁹ *Specification*, 4:14-21.

¹⁰ *Specification*, 11:1-19.

¹¹ *Specification*, 7:23-25.

¹² *Specification*, FIG. 4 ("O-DB"); 4:1-5; 5:1 (table).

¹³ *Specification*, 5:1 (table); *Specification*: 5-29-6:2.

¹⁴ *Id.*

¹⁵ *Id.*

outside of the table;¹⁶ and controlling access to data in the second column using the second cryptographic information stored outside of the table.¹⁷

The foregoing passages are representative only. Support for the foregoing claims can be found in numerous other locations in the specification.

(6) Grounds of Rejection

The grounds of rejection to be reviewed on appeal are:

1. Did the Examiner properly reject claims 18, 19, 21, 28, 29, 31, 33, 37, 41, 42, 48, 49, 56, 57, 59, 66-68, 70, 74, 75, 79, 80, 86, 87, and 94-99 as rendered obvious by *Thomson* in view of *Denning*?

2. Did the Examiner properly reject claims 32, 44, 51, 69, 82, and 89 as rendered obvious by *Thomson* in view of *Denning* and *Abraham*?

3. Did the Examiner properly reject claims 23-27, 34-36, 38-40, 45-47, 52-54, 61-65, 71-73, 76-78, 83-85 and 90-92 as rendered obvious by *Thomson* in view of *Denning* and *Gaskell*?

4. Did the Examiner properly reject claims 20, 22, 43, 50, 58, 60, 81 and 88 as rendered obvious by *Thomson* in view of *Denning* and *Pfleeger*?

5. Did the Examiner properly reject claim 30 as rendered obvious by *Thomson* in view of *Denning* and *Johansson*?

(7) Argument

I. OBVIOUSNESS

The burden is on the PTO to establish a prima facie showing of obviousness.¹⁸ A prima facie case of obviousness requires (1) a suggestion or motivation to combine; (2) a reasonable expectation of success;¹⁹ and (3) a teaching or suggestion of all claim limitations in the prior art.²⁰

There must be some logical reason apparent from the evidence or record to justify combination or modification of references.²¹ In addition, even if all of the claim elements are disclosed in various prior art references, the claimed invention taken as a whole cannot be said to

¹⁶ *Specification*, 6:2-16.

¹⁷ *Id.*

¹⁸ *In re Fritsch*, 972 F.2d 1260, 1265, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992).

¹⁹ *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1125 (Fed. Cir. 2000).

²⁰ *CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003).

²¹ *In re Regal*, 526 F.2d 1399, 1403 n.6, 188 U.S.P.Q.2d 136 (C.C.P.A. 1975).

be obvious without some reason given in the prior art why one of ordinary skill in the art would have been prompted to combine the teachings of the references to arrive at the claimed invention.²² Even if the cited references show the various elements suggested by the Examiner, in order to support a conclusion that it would have been obvious to combine the cited references, the references must either expressly or impliedly suggest the claimed combination or the Examiner must present a convincing line of reasoning as to why one skilled in the art would have found the claimed invention obvious in light of the teachings of the references.²³

II. CITED ART

A. *Thomson*

Thomson discloses a database system in which a user has access only to information with which the user is associated, for example, pertaining to his department or state.²⁴ When a user requests data from a table view in *Thomson*, the table view first looks up, in a security table, which data the user is authorized to access. For example, the table view may look up the user's state; or the user's department.²⁵ Next, the table view sends a query to the underlying table, requesting only rows matching the user's authorization. For example, the table view requests only rows whose "state" field matches the user's state, or whose "department" field matches the user's department.²⁶

Thus, *Thomson* discloses a quick security mechanism to ensure that a user has access only to those rows in a database that the user is authorized to access.²⁷ Data security is assured solely through the level of indirection afforded by the table view. *Thomson* does not describe any other form of data security, e.g., encryption.

B. *Denning*

Denning discloses a system that encrypts data on an element-by-element basis²⁸ without loss of security.²⁹ In one system disclosed by *Denning*, each data element is encrypted with a

²² *Id.*

²³ *Ex Parte Clapp*, 227 U.S.P.Q.2d 972, 973 (Board. Pat. App. & Inf. 1985).

²⁴ *Thomson*, FIGS 5 & 6 and associated text.

²⁵ *Thomson*, FIG. 3 and associated text.

²⁶ *Thomson*, FIGS. 5 & 6 and associated text.

²⁷ *Thomson*, 2:23-26.

²⁸ *Denning* refers to columns as fields, and cells within a given record as data elements. This Appeal Brief uses "field" and "column" interchangeably, and uses the term "element" to refer to data cells within a record.

²⁹ *Denning*, § 2.2, p. 233.

separate element key.³⁰ An element key is computed from a field key, which is a key common to an entire column of data. It does so by applying a cryptographic function to the field key in conjunction with an identifier uniquely specifying the particular record.³¹ The field key is computed by applying a cryptographic function to a master key in conjunction with an identifier uniquely specifying the column of data for which the field key is to be used.³² The sole use for the master key is to create field keys; and the sole use for the field keys is to create element keys.³³

Denning also describes a similar system in which, instead of being used to generate field keys, the master key is used to generate *record* keys. This is carried out by applying a cryptographic function to the master key and a unique record identifier. The record key is then used to generate an element key by applying a cryptographic function to the record key in conjunction with a field identifier.³⁴ *Denning* also describes a system in which the master key is used to directly create an element key (i.e., with no intervening field key or record key).³⁵

Each of these systems share a common attribute: the master key never actually encrypts data. It is only used to create further keys, whether they be field keys, record keys, or element keys.

Moreover, *Denning* does not disclose how the master key is derived, or how, where, or if, the master key is stored.

C. *Gaskell*

Gaskell discloses an improved method of authenticating a user to a computer system. Specifically, *Gaskell* explains how to improve a standard authentication system, called "Kerberos," by using smart cards instead of manual password entry.³⁶ Using the standard Kerberos authentication mechanism, the system prompts the user for a login name. The login name is sent to the authentication server, which responds by sending an encrypted "ticket granting ticket" (TGT). The user is prompted for a password, which is used to derive the user's

³⁰ *id.*

³¹ *id.*, § 2.3, p. 235-237.

³² *id.*

³³ *id.*

³⁴ *id.*, § 2.3, p. 237.

³⁵ *id.*, § 2.3, p.

³⁶ *Gaskell*, § 1.1, p. 1.

key. The user's key is then used only to decrypt the TGT. The decrypted TGT includes a limited-lifetime session key that may be used to request further system services.³⁷

Gaskell proposes improving this system by storing the user's key on the smart card (rather than deriving it from a password), and by performing some cryptographic operations on the smart card.³⁸

III. THOMSON AND DENNING FAIL TO RENDER OBVIOUS CLAIMS 18, 19, 21, 28, 29, 31, 33, 37, 41, 42, 48, 49, 56, 57, 59, 66-68, 70, 74, 75, 79, 80, 86, 87, AND 94-99

A. Thomson and Denning Fail to Disclose the Limitations of Claims 41, 42, 79, 80, 95, and 97

1. Denning Fails to Disclose Storing Second Cryptographic Information

The Examiner rejected claim 41 as rendered obvious by *Thomson* in view of *Denning*. However, neither *Thomson* nor *Denning* discloses "storing first and second cryptographic information outside of the table." The Examiner argues that *Denning* inherently discloses this element because *Denning*'s master key, according to the Examiner, must be stored outside the table³⁹.

Even if the Examiner were correct concerning the alleged inherent disclosure (*but see* section III.A.2, *infra*), *Denning* does not disclose storing *second* cryptographic information outside the table.

The Examiner appears to consider *Denning*'s field keys (or record keys, or element keys) to correspond to the claimed second cryptographic information *stored* outside the table.⁴⁰ But according to *Denning*, the field keys (and record keys and element keys) are *computed*, not stored. In *Denning*, each data element is encrypted using a distinct element key,⁴¹ which is *computed* from a field key (for the column). This field key is itself computed from a master key.⁴² For example, *Denning* discloses computing first a field key by encrypting, using the master key, a unique field identifier, then an element key by encrypting, now using this field key,

³⁷ *id.*

³⁸ *Id.*, § 2, p. 2.

³⁹ *Final Office Action*, ¶ 10.

⁴⁰ *Final Office Action*, ¶ 22.

⁴¹ *Denning*, § 2.2, p. 233.

⁴² *Denning*, § 2.3, p. 235.

a unique record identifier.⁴³ There is no need to store either the field key or the element key, since they are both easily calculated from the master key, the field identifier, and the record identifier. Thus, even if *Denning* disclosed storing cryptographic information, the only such information that would be stored would be the master key. *Denning* does not disclose, or suggest, storing *second* cryptographic information, as required by the claim.

2. *Denning* Fails to Inherently Disclose Storing Cryptographic Information Outside the Table

The Examiner has already conceded the absence of any express disclosure in *Denning* and *Thomson* of storing cryptographic information outside the table. Having done so, the Examiner now suggests that such disclosure is nevertheless implied. The Examiner's position is based on the notion that because the contents of the table are either encrypted or non-sensitive, it would make no sense to store the key in the table. Therefore, *Denning* inherently discloses storing the key separately from the table.

The Examiner's argument that *Denning* inherently discloses storing cryptographic information outside the table,⁴⁴ is flawed. A reference inherently discloses a feature only if the existence of that feature *necessarily* follows from the disclosure. However, if the absence of the feature is also consistent with the disclosure, then the reference fails to inherently disclose the feature. This statement of the law of inherency is articulated in MPEP 2112:

“[t]he fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic”

as well as by the Board of Appeals:

“In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic *necessarily* flows from the teachings of the applied prior art”⁴⁵

and again, nine years later, by the Federal Circuit itself:

To establish inherency, the extrinsic evidence “must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.”

⁴³ *Denning*, § 2.3, p. 235.

⁴⁴ *Final Office Action*, ¶ 10.

⁴⁵ *Ex parte Levy*, 17 USPQ 2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) [emphasis in original].

Continental Can Co. v. Monsanto Co., 948 F.2d 1264, 1268, 20 U.S.P.Q.2d 1746, 1749 (Fed.Cir.1991). “*Inherency, however, may not be established by probabilities or possibilities.* The mere fact that a certain thing may result from a given set of circumstances is not sufficient.” *Id.* at 1269, 948 F.2d 1264, 20 U.S.P.Q.2d at 1749 (quoting *In re Oelrich*, 666 F.2d 578, 581, 212 U.S.P.Q. 323, 326 (C.C.P.A.1981)).⁴⁶

The Examiner improperly relies on mere “probabilities or possibilities” when arguing that *Denning* inherently discloses storing a key outside the table. As the Examiner acknowledges, *Denning* does not explain *whether*, or *how*, the master key is stored.⁴⁷

A system according to *Denning*, in which the master key is stored *inside* the table, would be useful, for example, in a database system in which only two levels of access were permitted: administrator and user. The database administrator might have full confidence in the access control mechanism's ability to preclude intruders from logging in as “administrator,” perhaps because the administrator would only be permitted to log in from a local console. But the administrator might wish to restrict access to individual users. The solution, in this example, might be to store a *Denning* master key in the *same table* as the sensitive data, but to specify that it may only be accessed by an administrator. Then, the master key could be used in the manner specified by *Denning* to encrypt individual data elements within the rest of the table.

Appellant previously described a similar example to respond to the Examiner's “inherency” argument.⁴⁸ In response to this example, the Examiner states that *Denning* does not disclose any such example.⁴⁹ While this may be true, the same can be said about the Examiner's assertion that *Denning* inherently discloses storing the master key outside the table. And therein lies the flaw in the rejection. *Denning* is equally silent on both of these possibilities. But it is the Examiner who has the burden of establishing inherency. As stated in *In re Robertson*, “[t]he mere fact that a certain thing [storage outside the table] *may* result from a given set of circumstances [*Denning's* disclosure] is *not* sufficient.”⁵⁰ Appellant's point is not that *Denning* discloses the possibility that the key is stored outside the table, but rather that *Denning* could just as easily be said to “inherently disclose” this possibility. Appellant raises this possibility only to

⁴⁶ *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) [emphasis added].

⁴⁷ *Final Office Action*, ¶ 10.

⁴⁸ *Request for Reconsideration in Reply to Final Action of July 22, 2005*, § 2.1, p. 7.

⁴⁹ *Advisory Action* at 3.

⁵⁰ 169 F.3d 743, 745, 49 U.S.P.Q.2d 1949 (Fed.Cir. 1999) [emphasis added].

demonstrate two alternatives to the Examiner's proposal, neither of which require storing a master key outside the table. In doing so, Appellant demonstrates that the key need not *necessarily* be stored outside the table. Therefore, *Denning* fails to inherently disclose the element of storing cryptographic information outside the table.

3. Thompson Fails to Remedy the Deficiency in Denning's Disclosure

The Examiner concedes that *Thomson* does not disclose encryption at all.⁵¹ Accordingly, *Thomson* cannot remedy *Denning*'s failure to disclose storing first and second cryptographic information outside the table. Therefore, the combination of *Denning* and *Thomson* also fails to disclose or render obvious storing first and second cryptographic information outside of the table.

Claims 42-47, 94 and 95 depend on claim 41 and are patentable for at least the same reasons. Claim 79 contains similar limitations, and it, and its dependent claims 80-85 and 97, are also patentable for at least the same reasons.

B. THOMPSON AND DENNING FAIL TO RENDER OBVIOUS CLAIMS 18, 19, 21, 28, 29, 31, 33, 37, 48, 49, 56, 57, 59, 66-68, 70, 74, 75, 86, 87, 94, 96, 98, and 99

1. The Cited Art Fails to Disclose "Cryptographic Information Associated With" Data.

Independent claim 48 requires "information stored outside [a] table" including "cryptographic information associated with [an] encrypted column of data." As with claim 41, the Examiner argues that *Denning*'s alleged inherent disclosure of storing a master key outside a database table satisfies this limitation. In response, Appellant incorporates herein the argument set forth above (Section III.A.2.) in connection with *Denning*'s failure to inherently disclose storing a master key outside the table.

In addition, *Denning*'s master key is not "cryptographic information *associated with* [an] encrypted column of data." A master key in *Denning* is associated with an entire table, not with a column in the table.⁵² Although *Denning* discloses examples of tables with multiple columns, the master key is not associated with any of these columns—it is associated, instead, with the entire table. The particular key associated with an individual column (i.e., the "cryptographic

⁵¹ *Final Office Action*, ¶ 14.

⁵² *Denning*, § 2.3 explains that a master key is used to create a field key, record key, or element key. A field key or record key can also be used to create an element key. It is only the element key, not the master key, that is ultimately used to encrypt or decrypt data in the table.

information *associated with*" a column of data) must be calculated, in part on the basis of the master key.⁵³

A master key associated with an entire table cannot fairly be said to be associated with any one of its columns. As an analogy, consider a homeowner who has purchased a fire insurance policy. Following a fire, the homeowner files a claim with the insurance company, only to find that the policy, although "associated with" his home, did not cover a rare stamp collection in the attic. The insurance company draws attention to a rider that, had it been purchased, would have covered the stamp collection.

In this example, the disappointed homeowner's insurance policy corresponds to *Denning's* master key. Just as the insurance policy is "associated with" the home, the master key is "associated with" the entire table in *Denning*. But, just as the insurance policy is *not* "associated with" the rare stamp collection, *Denning's* master key is not "associated with" any particular column of data.

Had it been purchased, a policy rider *would* have been associated with the stamp collection. Similarly, in *Denning*, a field encryption key can be calculated that is associated with a particular column. In the context of the example, the rider is attached to the main policy, but it is the rider, not the main policy by itself, that is associated with the stamp collection. Similarly, in *Denning*, the field encryption key is derived from the master key (plus a unique field identifier), but it is the field encryption key, not the master key, that is associated with a particular column.⁵⁴

The Examiner concedes that *Thomson* does not disclose encryption at all.⁵⁵ Accordingly, *Thomson* cannot remedy *Denning's* failure to disclose the limitations discussed above. Therefore, the combination of *Denning* and *Thomson* also fails to disclose or render obvious storing cryptographic information associated with an encrypted column.

Claims 49-54 and 98 are dependent on claim 48 and are patentable for at least the same reasons. Claim 86 contains limitations similar to those of claim 48, and is patentable for at least

⁵³ *Denning*, § 2.3.

⁵⁴ Appellant does not suggest whether a system that stores encryption keys associated with *individual data elements* would or would not fall within the scope of the claims.

⁵⁵ *Final Office Action*, ¶ 14.

the same reasons. Claims 87-92 and 99 are dependent on claim 86 and are patentable for at least the same reasons.

2. The Cited Art Fails to Disclose Maintaining “Information for Controlling Access to a Specified Proper Subset” of Data.

Claims 18 and 56 require “maintaining, separate from the table of data, information for controlling access to a specified *proper subset*” of data.

The Examiner argues that *Thomson*'s maintenance of a security table corresponds to the above limitation. But the security table in *Thomson* restricts access to the *entire* table, not just to a proper subset thereof. In *Thomson*, an attempt to access *any* data in the table requires inspection of the security table to determine if the user is allowed access.⁵⁶

In other words, even if the security table could be viewed as corresponding to “maintaining, separate from the table of data, information for controlling access,” the security table does not include “information for controlling access to a specified proper subset of data. The only information in the security table is information for controlling access to the *entire* table of data.

Nor does *Denning*'s supposedly inherent disclosure of storing a master key from outside a database table correspond to “maintaining, separate from the table of data, information for controlling access to a specified *proper subset*” of data. As explained above in section III.B.1, the master key is not information associated with a *proper subset* of data in the table—it is associated with the *entire* table. The *field keys*, which are associated with individual fields, may be viewed as “information for controlling access to a specified proper subset.” But these field keys are *calculated* on an as-needed basis, not “maintained,” as the claim requires.

Therefore, the combination of *Denning* and *Thomson* also fails to disclose or render obvious the limitations of claim 18 and 56. Claims 19-40, 57-78, 94, and 96 depend on claims 18 and 56 and are patentable for at least the same reasons.

For reasons set forth above, Applicant submits that the Examiner improperly rejected claims 18 and 56, and all claims dependent thereon.

⁵⁶ *Thomson*, 4:60-64 (security table is used “to allow user access to authorized rows of the server TABLE1 based on the user ID's and row labels”).

IV. THOMSON, DENNING, AND ABRAHAM FAIL TO RENDER OBVIOUS CLAIMS 32, 44, 51, 69, 82, AND 89

A. Claim 32

The Examiner rejected claims 32 as rendered obvious by *Thomson* in light of *Denning* and *Abraham*.⁵⁷ Appellant submits that in addition to being patentable for at least the same reasons as claim 18, on which it depends, claim 32 is also patentable because *Abraham* fails to supply the limitations the Examiner concedes to be missing from *Thomson* and *Denning*.

In particular, claim 32 requires the additional limitation that “the information for controlling access,” which is maintained separately from the table, “comprises encrypted information.”

Appellant draws particular attention to *Abraham* at column 7, lines 45-48 which states:

Keys are stored on PC disk memory in encrypted form, encrypted under the master key of one of the security devices. [sic] cryptographic adapter 29, card reader 17, or IC card 19.⁵⁸

Abraham thus teaches storing encrypted keys on PC disk memory. This is not the same as teaching that encrypted keys are stored *separately* from the table. After all, the table itself is also likely to be stored in PC disk memory. *Abraham* is, at best, inconclusive concerning whether the encrypted key is stored *with* a table or *separately* from a table. Similarly, *Abraham* is inconclusive concerning whether the encrypted key is stored with any particular column of data in a table, or separately from any particular column of data.

The foregoing passage also suggests that *Abraham* stores, somewhere in a security device, a master key that is used to encrypt the keys that are ultimately stored in disk memory. However, this master key itself does not appear to be encrypted.

The Examiner suggests that the encrypted key must be stored separately from the table for reasons set forth in paragraph 9 of the final office action. In response, Appellant draws attention again to the counter-example described above (see section III.A.2) in connection with the discussion of inherency. Moreover, since the key is already stored in encrypted form, there would be no necessity to store it separately from the encrypted data, since a malicious user who gained access to the encrypted key would be unable to use it without the master key.

⁵⁷ U.S. Patent No. 5,148,481.

⁵⁸ *Abraham et al.*, U.S. Patent No. 5,148,481, col. 7, lines 45-48.

Appellant submits therefore that the section 103 rejection of the foregoing claims is improper because the proposed combination fails to disclose each and every limitation of the claimed invention. Applicant also maintains that the section 103 rejection is improper for the reasons discussed in connection with claim 18.

B. Claims 44 and 82

Claim 44 requires that “the first and second cryptographic information are stored, in encrypted form, outside of the table.” Claim 82 requires that “the first and second cryptographic information are stored, in encrypted form, outside of the first and second column.” As noted above (section IV.A), *Abraham* does not disclose storing encrypted information outside a table or outside a column. *Abraham* therefore fails to render claim 44 obvious, alone or in conjunction with *Denning* and *Thomson*.

In addition, claims 44 and 82 are patentable for at least the same reasons as claims 41 and 79, respectively (see section III.A).

C. Claims 51 and 89

Claim 51 requires that “information stored outside the table for controlling access to at least one column of data” be “stored in encrypted form.” Claim 89 requires that “information stored outside of the first column of data for controlling access to the first column of data” be “stored in encrypted form.” As noted above (section IV.A), *Abraham* does not disclose storing encrypted information outside a table or outside a column. *Abraham* therefore fails to render claim 51 obvious, alone or in conjunction with *Denning* and *Thomson*.

In addition, claim 51 is patentable for at least the same reasons as claim 48 (see section III.B.1). Claim 89 is patentable for at least the same reasons as claim 86 (see section III.B.1).

D. Claim 69

Claim 69 requires that information for controlling access, which is “maintain[ed] separate from [a] first set of data,” “comprises encrypted information.” As noted above (section IV.A), *Abraham* does not disclose storing encrypted information outside a table. *Abraham* therefore fails to render claim 51 obvious, alone or in conjunction with *Denning* and *Thomson*.

In addition, claim 69 is patentable for at least the same reasons as claim 56 (see section III.B.2).

E. Claim 82

Claim 82 requires that information for controlling access, which is “maintain[ed] separate from [a] first set of data,” “comprises encrypted information.” As noted above (section IV.A), *Abraham* does not disclose storing encrypted information outside a table. *Abraham* therefore fails to render claim 51 obvious, alone or in conjunction with *Denning* and *Thomson*.

In addition, claim 69 is patentable for at least the same reasons as claim 56 (see section III.B.2).

V. THOMSON, DENNING, AND GASKELL FAIL TO RENDER OBVIOUS CLAIMS 23-27, 34-36, 38-40, 45-47, 52-54, 61-65, 71-73, 76-78, 83-85 AND 90-92

The Examiner rejected dependent claims 23-27, 34-36, 38-40, 45-47, 52-54, 61-65, 71-73, 76-78, 83-85 and 90-92 as rendered obvious by *Thomson* in light of *Denning* and *Gaskell*.⁵⁹ Applicant maintains that these rejections are improper for the reasons set forth above with respect to the claims upon which each claim depends. In addition, *Gaskell* fails to disclose the additional elements set forth in these dependent claims.

A. Claims 23, 26-27, and 61

In particular, *Gaskell* discloses using a smart card to authenticate a user to a computer system using the Kerberos authentication method.⁶⁰ A properly-authenticated user will be able to decrypt a session key. The decrypted session key is used as a ticket to access services on the system.⁶¹

Claims 23 and 61 require that “controlling access to the *specified proper subset* of the data comprises using a tamper-resistant hardware module.” *Gaskell* discloses using a smart card to authenticate to *an entire system*, not a proper subset of data. Therefore, *Gaskell* fails disclose the additional limitations of claims 61, 23, or its dependent claims 26-27.

B. Claim 24

Claim 24 requires that the tamper-resistant hardware module be “used to perform a cryptographic operation on the data.” As recited in claim 18, from which claim 24 ultimately depends, this data is in a table in row and column format.

⁵⁹ *Gaskell et al.*, “Improved Security for Smart Card Use in DCE.”

⁶⁰ *Gaskell*, § 1.1, p. 1.

⁶¹ *id.*

Gaskell discloses that the smart card is used to decrypt a ticket-granting ticket (TGT). The Examiner apparently considers this TGT to be “the data” recited in claim 24. But the TGT is not data in a table “in row and column format,” as recited in the claim. It is simply stand-alone data that contains a key with a limited lifetime.⁶² Therefore, *Gaskell* fails to disclose the additional limitations of claim 24.

In addition, claim 24 is patentable at least for the reasons set forth above with respect to claims 18 and 23.

C. Claims 34-36

Claim 34 requires that “decrypting the data is done using a tamper-resistant hardware module.” According to claim 18, from which claim 34 ultimately depends, this data is contained in a table in row and column format.

Gaskell discloses that the smart card is used to decrypt a ticket-granting ticket (TGT). As with claim 24, the Examiner apparently considers this TGT to be “the data” recited in claim 34. But, as explained in connection with claim 24, the TGT is not data in a table in row and column format. Therefore, *Gaskell* fails to disclose the additional limitations of claim 34.

In addition, claim 34 is patentable at least for the reasons set forth above with respect to claim 18. Claims 35 and 36 are patentable for at least the same reasons as claim 34.

D. Claims 38-40

Claim 38 requires “decrypting the data from the particular data element using a tamper-resistant hardware module.” The “particular data element” contains encrypted data, and is in a table in row and column format.

As with claims 24 and 34, the Examiner appears to consider that the “particular data element” corresponds to the TGT in *Gaskell*. But *Gaskell* does not disclose that the TGT is stored in a table.⁶³ The TGT cannot, therefore, correspond to the “particular data element” of claim 38.

In addition, claim 38 is patentable for at least the reasons set forth above with respect to claims 37 and 18. Claims 39 and 40 are patentable for at least the same reasons as claim 38.

⁶² *Gaskell*, § 1.1, p. 1.

⁶³ *Gaskell*, § 1.1, p. 1.

E. Claims 52-54 and 90-92

Claims 52 and 90 require a tamper-resistant hardware module for performing cryptographic operations on an encrypted column of data. Claim 52 requires that the data be in a table with at least two columns of data. Claim 90 requires that the data be in a database with at least two columns of data.

As with the preceding claims, the Examiner apparently considers the TGT to correspond to “the data” recited in claims 52 and 90. But, the TGT is not data in a table or database with at least two columns of data.⁶⁴ Therefore, *Gaskell* fails to disclose the additional limitations of claim 24.

In addition, claim 52 is patentable at least for the reasons set forth above with respect to claim 48. Claims 53-54 are patentable for at least the same reasons as claim 52. Claim 90 is also patentable for at least the same reasons as claim 86. Claims 91-92 are patentable for at least the same reasons as claim 90.

F. Claims 62-65

Claim 62 requires that the tamper-resistant hardware module be “used to perform a cryptographic operation on the data,” the data being maintained as a collection of records having fields.

The Examiner apparently considers the TGT to correspond to “the data” recited in claim 62. But the TGT is simply stand-alone data.⁶⁵ *Gaskell* does not disclose that it is maintained as a collection of records having fields. Therefore, *Gaskell* fails to disclose the additional limitations of claim 62.

In addition, claim 62 is patentable at least for the reasons set forth above with respect to claims 61 and 56. Claims 63-65 are patentable for at least the same reasons as claim 62.

G. Claims 71-73 and 76-78

Claims 71 and 76 requires that “decrypting the data is done using a tamper-resistant hardware module.” The data is maintained as a collection of records having fields.

⁶⁴ *Gaskell*, § 1.1, p. 1.

⁶⁵ *Gaskell*, § 1.1, p. 1.

The Examiner apparently considers the TGT to correspond to "the data" recited in claims 71 and 76. But the TGT is not data maintained as a collection of records having fields.⁶⁶ Therefore, *Gaskell* fails to disclose the additional limitations of claims 71 and 76.

In addition, claims 71 and 76 are patentable at least for the reasons set forth above with respect to claim 70 and 56. Claims 72-73 are patentable for at least the same reasons as claim 71. Claim 76 is also patentable for at least the same reasons as claim 75. Claims 77 and 78 are patentable for at least the same reasons as claim 76.

H. Claim 25

Claim 25 requires that the tamper-resistant hardware be "used to store at least a portion of the separately maintained information."

Gaskell discloses that a smart card stores a key which is used to decrypt a TGT. The Examiner appears to consider the key stored on the smart card to correspond to a portion of the separately-maintained information. But the claim requires that the separately-maintained information be used to control access to a "specified proper subset" of data. By contrast, in *Gaskell*, the key in the smart card is used to authenticate to the entire system. Therefore, *Gaskell* does not disclose the additional limitations of claim 25.

In addition, claim 24 is patentable at least for the reasons set forth above with respect to claims 18, and 23.

I. Claims 45-47 and 83-85

Claims 45 and 83 require that "at least a portion of the data" be encrypted using a tamper-resistant hardware module. For claim 45, the data is in a table with at least two columns. For claim 83, the data is in a database with at least two columns.

The Examiner appears to consider that "the data" corresponds to the session key that is encrypted in the TGT in *Gaskell*. But *Gaskell* contains no disclosure that the key is in a table or database with at least two columns. Indeed, *Gaskell* explicitly states that the key has a limited lifetime, suggesting that it may be created on the fly rather than being stored in a table or database. Therefore, *Gaskell* fails to teach the additional limitations of claims 45 or 83.

⁶⁶ *Gaskell*, § 1.1, p. 1.

In addition, claim 45 is patentable for at least the reasons set forth above with respect to claim 41. Claims 46-47 are patentable for at least the same reasons as claim 45. Claim 83 is patentable for at least the reasons set forth above with respect to claim 79. Claims 84-85 are patentable for at least the same reasons as claim 83.

The claims argued in this section do not stand and fall together, since if the Board upholds Appellant's position with respect to an independent claim argued above, then each of that claim's dependent claims are patentable for at least the same reasons.

VI. *DENNING, THOMSON, AND PFLEEGER* FAIL TO RENDER OBVIOUS CLAIMS 20, 22, 43, 50, 58, 60, 81 AND 88

The Examiner rejected claims 20, 22, 43, 50, 58, 60, 81, and 88 as obvious in view of *Denning, Thomson, and Pfleeger*. Appellant submits, however, that these dependent claims are patentable for at least the same reasons as the claims upon which they depend. Claims 20 and 22 are patentable for at least the same reasons as claim 18 (see section III.B, above); claim 43 is patentable for at least the same reasons as claim 41 (see section III.A, above); claim 50 is patentable for at least the same reasons as claim 48 (see section III.B, above); claims 58 and 60 are patentable for at least the same reasons as claim 56 (see section III.B, above); claim 81 is patentable for at least the same reasons as claim 79 (see section III.A, above); and claim 88 is patentable for at least the same reasons as claim 86 (see section III.A, above).

VII. *DENNING, THOMSON, AND JOHANSSON* FAIL TO RENDER OBVIOUS CLAIM 30

The Examiner rejected claim 30 as obvious in view of *Denning, Thomson, and Johansson*. Appellant submits, however, that claim 30 is patentable for at least the same reasons as claims 29 and 18 (see section III.A, above).

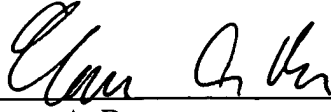
The brief fee of \$250 is enclosed. Please apply any other charges or credits to Deposit Account No. 06-1050.

Applicant : Ulf Dahl
Serial No. : 09/840,188
Filed : April 24, 2001
Page : 20 of 33

Attorney's Docket No.: 17299-008002

Respectfully submitted,

Date: 1/30/06



Thomas A. Brown
Reg. No. 54,619

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

Appendix of Claims

1-17. (Canceled)

18. (Previously Presented) A data processing method comprising:

maintaining a database containing a table of data in row and column format, at least a portion of the data being encrypted;

maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table; and

controlling access to the specified proper subset of data in the table according to the separately maintained information.

19. (Previously Presented) The method of claim 18, wherein controlling access comprises controlling access by a specified user or group of users.

20. (Previously Presented) The method of claim 18, wherein controlling access comprises controlling access by a specified program or group of programs.

21. (Previously Presented) The method of claim 18, wherein the separately maintained information comprises a separate table inaccessible to a user seeking access to the data.

22. (Previously Presented) The method of claim 18, wherein the separately maintained information comprises a separate table inaccessible to a program seeking access to the data.

23. (Previously Presented) The method of claim 18, wherein controlling access to the specified proper subset of the data comprises using a tamper-resistant hardware module.

24. (Previously Presented) The method of claim 23, wherein the tamper-resistant hardware module is used to perform a cryptographic operation on the data.

25. (Previously Presented) The method of claim 23, wherein the tamper-resistant hardware module is used to store at least a portion of the separately maintained information.

- 26. (Previously Presented)** The method of claim 23, wherein the tamper-resistant hardware module comprises a hardware security module.
- 27. (Previously Presented)** The method of claim 23, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.
- 28. (Previously Presented)** The method of claim 18, wherein the specified proper subset of data comprises a specified column of data.
- 29. (Previously Presented)** The method of claim 18, wherein the information for controlling access comprises information used in encrypting or decrypting data in the proper subset of data.
- 30. (Previously Presented)** The method of claim 29, wherein the information used in encrypting or decrypting data comprises information identifying a way of encrypting or decrypting data in the proper subset of data.
- 31. (Previously Presented)** The method of claim 18, wherein the information for controlling access comprises information identifying an owner of the proper subset of data.
- 32. (Previously Presented)** The method of claim 18, wherein the information for controlling access comprises encrypted information.
- 33. (Previously Presented)** The method of claim 18, further comprising:
- receiving a request for access to a particular data element in the table, the particular data element containing encrypted data;
 - obtaining, from the separately maintained data, cryptographic information associated with a proper subset of data in the table, the proper subset containing the particular data element; and
 - decrypting the data in the particular data element using the cryptographic information.

34. (Previously Presented) The method of claim 33, wherein decrypting the data is done using a tamper-resistant hardware module.

35 (Previously Presented) The method of claim 34, wherein the tamper-resistant hardware module comprises a hardware security module.

36. (Previously Presented) The method of claim 34, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

37. (Previously Presented) The method of claim 18, further comprising

receiving a request for access to a particular data element in the table, the particular data element containing encrypted data; and

obtaining, from the separately maintained data, information associated with a proper subset of data in the table, the proper subset containing the particular data element; and

providing decrypted data from the particular data element when the information from the separately maintained data indicates that the request for access to the particular data element is an authorized request.

38. (Previously Presented) The method of claim 37, further comprising decrypting the data from the particular data element using a tamper-resistant hardware module.

39. (Previously Presented) The method of claim 38, wherein the tamper-resistant hardware module comprises a hardware security module.

40. (Previously Presented) The method of claim 38, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

41. (Previously Presented) A method comprising:

providing a database containing a table having at least two columns of data;

encrypting data in a first column using first cryptographic information;

encrypting data in a second column using second cryptographic information;

storing first and second cryptographic information outside of the table;

controlling access to data in the first column using the first cryptographic information stored outside of the table; and

controlling access to data in the second column using the second cryptographic information stored outside of the table.

- 42. (Previously Presented)** The method of claim 41, further comprising storing the first and second cryptographic information in a separate table inaccessible to a user seeking access to the data.
- 43. (Previously Presented)** The method of claim 41, further comprising storing the first and second cryptographic information in a separate table inaccessible to a program seeking access to the data.
- 44. (Previously Presented)** The method of claim 41, wherein the first and second cryptographic information are stored, in encrypted form, outside of the table.
- 45. (Previously Presented)** The method of claim 41, wherein at least a portion of the data is encrypted using a tamper-resistant hardware module.
- 46. (Previously Presented)** The method of claim 45, wherein the tamper-resistant hardware module comprises a hardware security module.
- 47. (Previously Presented)** The method of claim 45, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

48. (Previously Presented) A database management system comprising:

a database containing a table having at least two columns of data, at least one column of data being encrypted; and

information stored outside of the table for controlling access to at least one column of data, the information including cryptographic information associated with the encrypted column of data.

49. (Previously Presented) The system of claim 48, wherein the information is stored in a separate table inaccessible to a user seeking access to the data.

50. (Previously Presented) The system of claim 48, wherein the information is stored in a separate table inaccessible to a program seeking access to the data.

51. (Previously Presented) The system of claim 48, wherein the information is stored in encrypted form.

52. (Previously Presented) The system of claim 48, further comprising a tamper-resistant hardware module for performing cryptographic operations on the encrypted column of data.

53. (Previously Presented) The system of claim 52, wherein the tamper-resistant hardware module comprises a hardware security module.

54. (Previously Presented) The system of claim 52, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

55. (Cancelled)

56. (Previously Presented) A data processing method comprising:

maintaining a first set of data as a collection of records having fields, at least a portion of the data being encrypted;

maintaining, separate from the first set of data, information for controlling access to a specified proper subset of the first data; and

controlling access to the specified proper subset of the first set of data according to the separately maintained information.

57. (Previously Presented) The method of claim 56, wherein controlling access comprises controlling access by a specified user or group of users.

58. (Previously Presented) The method of claim 56, wherein controlling access comprises controlling access by a specified program or group of programs.

59. (Previously Presented) The method of claim 56, wherein the separately maintained information comprises information that is inaccessible to a user seeking access to the data.

60. (Previously Presented) The method of claim 56, wherein the separately maintained information comprises information that is inaccessible to a program seeking access to the data.

61. (Previously Presented) The method of claim 56, wherein controlling access to the specified proper subset of the data comprising using a tamper-resistant hardware module.

62. (Previously Presented) The method of claim 61, wherein the tamper-resistant hardware module is used to perform a cryptographic operation on the data.

63. (Previously Presented) The method of claim 61, wherein the tamper-resistant hardware module is used to store at least a portion of the separately maintained information.

64. (Previously Presented) The method of claim 61, wherein the tamper-resistant hardware module comprises a hardware security module.

- 65. (Previously Presented)** The method of claims **61**, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.
- 66. (Previously Presented)** The method of claim **56**, wherein the specified proper subset of data comprises a specified field of data.
- 67. (Previously Presented)** The method of claim **56**, wherein the information for controlling access comprises information used in encrypting or decrypting data in the proper subset of data.
- 68. (Previously Presented)** The method of claim **56**, wherein the information for controlling access comprises information identifying an owner of the proper subset of data.
- 69. (Previously Presented)** The method of claim **56**, wherein the information for controlling access comprises encrypted information.
- 70. (Previously Presented)** The method of claim **56**, further comprising:
- receiving a request for access to a particular data element in the first set of data, the particular data element containing encrypted data;
 - obtaining, from the separately maintained data, cryptographic information associated with a proper subset of the first set of data, the proper subset containing the particular data element; and
 - decrypting the data in the particular data element using the cryptographic information.
- 71. (Previously Presented)** The method of claim **70**, wherein decrypting the data is done using a tamper-resistant hardware module.
- 72. (Previously Presented)** The method of claim **71**, wherein the tamper-resistant hardware module comprises a hardware security module.

73. (Previously Presented) The method of claim 71, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

74. (Previously Presented) The method of claim 70, wherein the proper subset comprises data in one or more specified fields.

75. (Previously Presented) The method of claim 56, further comprising

receiving a request for access to a particular data element in the first set of data, the particular data element containing encrypted data; and

obtaining, from the separately maintained data, information associated with a proper subset of data in the first set of data, the proper subset containing the particular data element; and

providing decrypted data from the particular data element when the information from the separately maintained data indicates that the request for access to the particular data element is an authorized request.

76. (Previously Presented) The method of claim 75, further comprising decrypting the data from the particular data element using a tamper-resistant hardware module.

77. (Previously Presented) The method of claim 76, wherein the tamper-resistant hardware module comprises a hardware security module.

78. (Previously Presented) The method of claim 76, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

79. (Previously Presented) A method comprising:

providing a database containing at least two columns of data;

encrypting data in a first column using first cryptographic information;

encrypting data in a second column using second cryptographic information;

storing the first and second cryptographic information apart from the two columns of data;

controlling access to data in the first column using the first cryptographic information;
and

controlling access to data in the second column using the second cryptographic information.

80. (Previously Presented) The method of claim 79, further comprising storing the first and second cryptographic information in a location that is inaccessible to a user seeking access to the data.

81. (Previously Presented) The method of claim 79, further comprising storing the first and second cryptographic information in a location that is inaccessible to a program seeking access to the data.

82. (Previously Presented) The method of claim 79, wherein the first and second cryptographic information are stored, in encrypted form, outside of the first and second column.

83. (Previously Presented) The method of claim 79, wherein at least a portion of the data is encrypted using a tamper-resistant hardware module.

84. (Previously Presented) The method of claim 83, wherein the tamper-resistant hardware module comprises a hardware security module.

85. (Previously Presented) The method of claim 83, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

86. (Previously Presented) A database management system comprising:

a database containing at least two columns of data, a first column of data being encrypted; and

information stored outside of the first column of data for controlling access to the first column of data, the information including cryptographic information associated with the first column of data.

87. (Previously Presented) The system of claim 86, where in the information is stored in a location that is inaccessible to a user seeking access to the first column of data.

88. (Previously Presented) The system of claim 86, where in the information is stored in a location that is inaccessible to a program seeking access to the first column of data.

89. (Previously Presented) The system of claim 86, wherein the information is stored in encrypted form.

90. (Previously Presented) The system of claim 86, further comprising a tamper-resistant hardware module for performing cryptographic operations on the first column of data.

91. (Previously Presented) The system of claim 90, wherein the tamper-resistant hardware module comprises a hardware security module.

92. (Previously Presented) The system of claim 90, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

93. (Cancelled)

94. (Previously Presented) The method of claim 18, further comprising revealing an unauthorized access to the data.

95. (Previously Presented) The method of claim 41, wherein controlling access to data in the first column comprises revealing unauthorized access to the data.

96. (Previously Presented) The method of claim 56, wherein controlling access comprising revealing unauthorized access to the first set of data.

97. (Previously Presented) The method of claim 79, wherein controlling access to data in the first columns comprises revealing unauthorized access to the data.

98. (Previously Presented) The system of claim 48, wherein the information stored outside of the table comprises information for revealing unauthorized access to the database.

99. (Previously Presented) The system of claim 86, wherein the information stored outside of the table comprises information for revealing unauthorized access to the database.

Applicant : Ulf Dahl
Serial No. : 09/840,188
Filed : April 24, 2001
Page : 32 of 33

Attorney's Docket No.: 17299-008002

Appendix of Evidence

Applicant : Ulf Dahl
Serial No. : 09/840,188
Filed : April 24, 2001
Page : 33 of 33

Attorney's Docket No.: 17299-008002

Appendix of Related Proceedings